UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE ACCOUNT andrewgrillo6@gmail.com THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC	Case No. 24-mj-26-01-AJ **Filed Under Seal – Level II**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Deputy U.S. Marshal Brandon Wilson, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with the account andrewgrillo6@gmail.com that is stored at premises owned, maintained, controlled or operated by Google LLC ("Google"), an electronic communications service and/or remote computing service provider headquartered at 1600 Amphitheater Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.
2. I, Brandon Wilson, am a Deputy United States Marshal (DUSM) with the United States Marshals Service (USMS) and have been so employed for fourteen years. Prior to that I

was a Police Officer in Williston, Vermont for approximately five years. I am currently assigned to the U.S. Marshals Office for the District of New Hampshire. I have successfully completed the U.S. Marshals Basic Training Academy and the Criminal Investigator Training Program in Glynco, Georgia. I have participated in numerous fugitive and criminal investigations and, among other things, have conducted or participated in surveillance, execution of search warrants and other law enforcement investigations. Through my training, education and experience I have familiarized myself with the way fugitives or targets of criminal investigations utilize resources, including cellular telephones, social media accounts and emails to communicate while avoiding detection by law enforcement. I have also attended a three-day course designed specifically for the interpretation of electronic and cellular information to be used in the criminal investigations and apprehension of fugitives.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 912: Impersonation of an officer or employee of the United States, have been committed by unknown persons. There is also probable cause to search the information described in Attachment A for evidence of these violations, further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711 and 18 U.S.C. §§ 2703(a),

(b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated," 18 U.S.C. § 2711(3)(A)(ii).

PROBABLE CAUSE

6. On February 6, 2024, USMS, District of New Hampshire (D/NH), learned of an individual, reported to be impersonating a DUSM, specifically DUSM Andrew Grillo, who is currently a deputy with the D/NH. The USMS received reports of two phone calls placed to private citizens or businesses where the caller claimed to be a Deputy U.S. Marshal named "Andy Grillo."

7. On February 9, 2024, the D/NH Chief Deputy U.S. Marshal (CDUSM) was made aware of a third reporting party, who advised that she had received a suspicious call from an individual claiming to be DUSM Grillo. The CDUSM contacted the third reporting party, who informed the CDUSM that she received a call from the impersonator at her place of employment. The impersonator called, asked for the reporting party by name, and informed her that she had two "felony arrest warrants" for failure to appear for a summons. The reporting party informed the impersonator that she had not received a summons and asked what address the summons had been mailed to. The impersonator provided an address that was unfamiliar to the reporting party. The reporting party later asked to see a copy of the summons.

8. The reporting party gave the impersonator her email address, and the impersonator sent her a copy of a document that appears on its face to be a jury duty summons for the U.S. District Court, District of New Hampshire. The reporting party later forwarded this email to the CDUSM. The bottom of the forwarded document requests a variety of personal biographical information.

9. Based on a review of this forwarded email, the impersonator initially sent the summons from the email address andrewgrillo6@gmail.com (user name "Andrew Grillo") to the email address u.s.warrantdivision@mailfence.com (user name "Gary Schofield"). It should be noted that Mailfence is a company that provides encrypted email services and that Gary Schofield is presently the U.S. Marshal for the District of Nevada. The impersonator then forwarded the message via the Mailfence account to the reporting party.
10. The reporting party became suspicious and ultimately asked the impersonator to speak with his supervisor. A "supervisor" then introduced himself as "William," stated that there had been a "misunderstanding," and ended the call.
11. Since February 9, 2024, there have been multiple additional reports of persons receiving suspicious calls from an individual claiming to be DUSM Andy Grillo.

BACKGROUND CONCERNING GOOGLE

12. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.
13. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile

phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

14. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

15. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

16. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser,

their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

17. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. It a user is paying for services; the user must also provide a physical address and means and source of payment.

18. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

19. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

20. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

21. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation.

22. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

23. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, internet activity, documents, and contact can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

24. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

25. Based on the forgoing, I request that the court issue the proposed search warrant.

26. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

/s/ Brandon Wilson
Deputy United States Marshal
United States Marshals Service

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: **Feb 14, 2024**
Time: **5:19 PM, Feb 14, 2024**

HONORABLE ANDREA K. JOHNSTONE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Google account identifier andrewgrillo6@gmail.com (the "Account") that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC ("Google")

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, Google is required to disclose to the government for each account or identifier listed in Attachment A the following information from **December 12, 2023,** to **February 14, 2024**, unless otherwise indicated:

a. All business records and subscriber information, in any form kept, pertaining to the Account, including:

1. Names (including subscriber names, user names, and screen names);

2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);

3. Telephone numbers, including SMS recovery and alternate sign-in numbers;

4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, including log-in IP addresses;

5. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers

6. Length of service (including start date and creation IP) and types of service utilized;

7. Means and source of payment (including any credit card or bank account number); and

8. Change history.

b. All device information associated with the Account, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;

c. Records of user activity for each connection made to or from the Account(s), including, for all Google services, the date, time, length, and method of connection, data transfer volume, user names, source and destination IP address, name of accessed Google service, and all activity logs

Google is hereby ordered to disclose the above information to the government within **14 DAYS** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 912: Impersonating an officer or employee of the United States, including, for each Account or identifier listed on Attachment A, information pertaining to the following matters:

a. The impersonation of Deputy U.S. Marshal Andrew Grillo, U.S. Marshal Gary Schofield, or any other U.S. Marshals Service employee or other federal law enforcement officer;

b. Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

c. Evidence indicating the Account owner's state of mind as it relates to the crime under investigation; and

d. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).